**PCT** WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

| | | |
|---|---|---|
| (51) International Patent Classification 6 : **H04Q** | **A2** | (11) International Publication Number: **WO 99/01990**<br>(43) International Publication Date: 14 January 1999 (14.01.99) |

(21) International Application Number: PCT/FI98/00532

(22) International Filing Date: 18 June 1998 (18.06.98)

(30) Priority Data:
972819 30 June 1997 (30.06.97) FI

(71) Applicant *(for all designated States except US)*: SONERA OY [FI/FI]; Sturenkatu 16, FIN–00510 Helsinki (FI).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: VATANEN, Harri [FI/FI]; Sonera Oy, Sturenkatu 16, FIN–00510 Helsinki (FI).

(74) Agent: PAPULA REIN LAHTELA OY; Fredrikinkatu 61 A, P.O. Box 981, FIN–00101 Helsinki (FI).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

**Published**
*Without international search report and to be republished upon receipt of that report.*

(54) Title: PROCEDURE FOR SETTING UP A SECURE SERVICE CONNECTION IN A TELECOMMUNICATION SYSTEM

(57) Abstract

Procedure for setting up a secure service connection in a telecommunication system comprising a first telecommunication network (1), a first terminal device (2) connected to the first telecommunication network, a second telecommunication network (3), a second terminal device (4) connected to the second telecommunication network, and a telecommunication server (5), in which procedure the first terminal device is connected via a first telecommunication connection (6) to the telecommunication server and the second terminal device is connected to the telecommunication server via a second telecommunication connection (7). In an embodiment of the invention, the unique address of the first terminal device (2) and the data needed for the verification of information giving the first terminal device (2) access to the services of the telecommunication server (5) are transmitted via the second terminal device (4); the data sent by the second terminal device are verified in the telecommunication server, and the first telecommunication connection (6) from the telecommunication server to the first terminal device is set up based on the verification and the address data received if the first terminal device has the required right of access to the services of the telecommunication server.

*FOR THE PURPOSES OF INFORMATION ONLY*

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **AL** | Albania | **ES** | Spain | **LS** | Lesotho | **SI** | Slovenia |
| **AM** | Armenia | **FI** | Finland | **LT** | Lithuania | **SK** | Slovakia |
| **AT** | Austria | **FR** | France | **LU** | Luxembourg | **SN** | Senegal |
| **AU** | Australia | **GA** | Gabon | **LV** | Latvia | **SZ** | Swaziland |
| **AZ** | Azerbaijan | **GB** | United Kingdom | **MC** | Monaco | **TD** | Chad |
| **BA** | Bosnia and Herzegovina | **GE** | Georgia | **MD** | Republic of Moldova | **TG** | Togo |
| **BB** | Barbados | **GH** | Ghana | **MG** | Madagascar | **TJ** | Tajikistan |
| **BE** | Belgium | **GN** | Guinea | **MK** | The former Yugoslav Republic of Macedonia | **TM** | Turkmenistan |
| **BF** | Burkina Faso | **GR** | Greece | | | **TR** | Turkey |
| **BG** | Bulgaria | **HU** | Hungary | **ML** | Mali | **TT** | Trinidad and Tobago |
| **BJ** | Benin | **IE** | Ireland | **MN** | Mongolia | **UA** | Ukraine |
| **BR** | Brazil | **IL** | Israel | **MR** | Mauritania | **UG** | Uganda |
| **BY** | Belarus | **IS** | Iceland | **MW** | Malawi | **US** | United States of America |
| **CA** | Canada | **IT** | Italy | **MX** | Mexico | **UZ** | Uzbekistan |
| **CF** | Central African Republic | **JP** | Japan | **NE** | Niger | **VN** | Viet Nam |
| **CG** | Congo | **KE** | Kenya | **NL** | Netherlands | **YU** | Yugoslavia |
| **CH** | Switzerland | **KG** | Kyrgyzstan | **NO** | Norway | **ZW** | Zimbabwe |
| **CI** | Côte d'Ivoire | **KP** | Democratic People's Republic of Korea | **NZ** | New Zealand | | |
| **CM** | Cameroon | | | **PL** | Poland | | |
| **CN** | China | **KR** | Republic of Korea | **PT** | Portugal | | |
| **CU** | Cuba | **KZ** | Kazakstan | **RO** | Romania | | |
| **CZ** | Czech Republic | **LC** | Saint Lucia | **RU** | Russian Federation | | |
| **DE** | Germany | **LI** | Liechtenstein | **SD** | Sudan | | |
| **DK** | Denmark | **LK** | Sri Lanka | **SE** | Sweden | | |
| **EE** | Estonia | **LR** | Liberia | **SG** | Singapore | | |

PROCEDURE FOR SETTING UP A SECURE SERVICE CONNECTION IN A TELECOMMUNICATION SYSTEM

The present invention relates to a procedure as defined in the preamble of claim 1 for setting up of a secure service connection in a telecommunication system, which may comprise e.g. the Internet and a telephone network or mobile communication network.

The global data network, the Internet, is based on an open structure which practically anyone can join. In the network, each device included in the network has an individual name, an Internet name. The data link protocol used for communication over the Internet is TCP/IP (Transmission Control Protocol/Internet Protocol), in which TCP corresponds to OSI layer 4 and IP to layer 3. OSI (Open System Interconnection Architecture) is a standard defining how systems can be openly interconnected. In the OSI model, telecommunication software is divided into sections called layers. The principle is that the functions of the layer have been defined but the manner of implementation has been left open. For each layer, a specific interface has been defined, through which it communicates with the layers above and below it. The functions of a layer and those of the layers below it are called services.

A common problem restricting the use of the Internet is that the security of certain network layers consistent with the OSI model has not been standardised or otherwise defined. Therefore, a connection set up via the Internet between two computers or equivalent terminals is unprotected, which means that in principle anyone who is connected to the network can receive messages sent between the two computers and read them. Correspondingly, anyone can send messages intended for someone else via a connection between two computers and thus disturb or otherwise impair the

security and privacy of users. For example, placing orders and making payments for services sold via the Internet is difficult. Likewise, reliable user identification and connection setup are difficult and call for special arrangements

In wired telephone networks and in mobile communication networks, advanced methods for encrypting a telecommunication connection or at least the data transmitted over the connection are used. Especially in a mobile communication network such as the GSM network, the encryption of radio communication can be regarded as providing a very high level of security. Moreover, the GSM network standard allows the transmission of SMS or ESMS messages, so the information to be encrypted can be enciphered into the message at the transmitting end and deciphered at the receiving end. Such an arrangement can be regarded as providing a very high level of data security.

Patent specification WO 94/11849 presents a mobile communication system in which the user of the system is authenticated locally, whereupon a secure connection is set up to a service provider or a telecommunication server. However, a problem in selling services and offering them via a telephone network or mobile communication network is that the service provider has no way e.g. to graphically present the services or products in question. In addition, using or ordering services via a terminal in a telephone network or mobile communication network, i.e. via a telephone, is difficult.

The object of the present invention is to eliminate the problems referred to above.

A specific object of the present invention is to disclose a new type of procedure in a telecommunication system comprising both a telephone network and a data network, which procedure allows reliable user

identification and provides a handy and easy way for the user to order services offered by the network.

A further object of the present invention is to disclose a procedure in which the user can use or order products or services provided via the Internet regardless of his/her location and terminal device or computer connected to the Internet.

As for the features characteristic of the present invention, reference is made to the claims.

In the procedure of the invention for setting up a secure service connection in a telecommunication system comprising a first telecommunication network, preferably a data network or the Internet, a first terminal device, preferably a computer or equivalent, connected to the first telecommunication network, a second telecommunication network, preferably a telephone network and/or mobile communication network, and a second terminal device, preferably a telephone or mobile station, connected to the second telecommunication network, and a telecommunication server communicating with both the first and the second telecommunication networks, the first terminal device is connected via a first telecommunication connection to the telecommunication server and the second terminal device is connected via a second telecommunication connection to the telecommunication server.

According to the invention, the unique address of a computer in a data network or in the Internet as well as the data needed for the verification of information giving the computer access to the services of the telecommunication server, such as the user identifier and password, are transmitted via a telephone or mobile station. The data thus sent are verified in the telecommunication server and a first telecommunication connection from the telecommunication server to the first terminal device is set up based on the verification and the address data received if the

first terminal device or its user has the required right of access to the services of the telecommunication server. The access right may also comprise a given sum of money used to buy service time at the telecommunication server or the access right may consist of a command to open a connection, in which case the command to close the connection is sent in a corresponding manner via the telephone or mobile station. The unique address may be the IP address or domain name of the computer.

As compared with prior art, the present invention has the advantage that it makes it easy to verify the Internet user's right of access to services offered in the network and to pay for the services and products sold via the Internet. A further advantage of the invention as compared with prior art is that the user is not tied to a given computer or other corresponding data network terminal because the IP address from which the user is accessing the network is specified each time a connection is set up.

In an embodiment of the present invention, the second telecommunication connection to be established via a telephone network is set up as a secure connection in which all data transmitted via the connection is encrypted using a predetermined encrypting algorithm. Correspondingly, the data transmitted is decrypted in the telecommunication server and the data to be transmitted to the telephone is encrypted. On the other hand, the second telecommunication connection may also be a message switching connection, preferably an ESMS connection, in which case the connection is used to transmit encrypted message packets containing the above-mentioned address data and access right verification data.

In an embodiment of the invention, a check is carried out in the telecommunication server to establish whether the first and/or the second telecommu-

nication connection is active and whether the user has a right of access to the services provided via the telecommunication server. In this case, the payments for the service and connection may be charged on the basis of duration of connection.

In an embodiment of the invention, a fixed payment for the service is sent by telephone to the telecommunication server using e.g. known chargeable service number applications and the first telecommunication connection is disconnected on expiration of the service time corresponding to the payment.

In an embodiment, both connections are used in real time to buy a product or service via the Internet by sending a purchase order via the first telecommunication connection and the computer and reserving the purchase price on the user's account via the second telecommunication connection and the telephone. Next, the telecommunication server is informed of the reservation of the purchase price, and when the user receives the product or service and accepts it, the transaction is acknowledged by telephone, whereupon the reserved sum is transferred to the seller.

In the following, the invention will be described by the aid of a few preferred embodiments by referring to the attached drawing, which presents a telecommunication system according to the invention.

The drawing presents an example of a telecommunication system in which the procedure of the invention can be implemented. The telecommunication system shown in the drawing comprises the Internet 1 and a GSM telephone network 3. Moreover, a computer 2 is connected to the Internet and a mobile station 4 is connected to the GSM network. The service provider's telecommunication server 5 is connected both to the Internet and to the GSM network, and the computer 2 is connected via telecommunication connection 6 over the Internet to the telecommunication server while the mo-

bile station is connected to the telecommunication server via telecommunication connection 7 over the GSM network.

It is to be noted that the networks and terminal devices presented here are only examples and that other devices and networks applicable can also be used in the procedure of the invention.

The basic idea of the procedure of the invention is that an open network, such as the Internet 1, is used as a marketing and service channel in which products and services are presented, and the payments for desired products and services are made using a telephone via a separate telecommunication connection 7.

The Internet user, for whom a unique IP address has been defined, sets up a connection to the telecommunication server 5 from his/her computer after he/she has either sent from the mobile station 4 a payment message, e.g. an ESMS message containing his/her user identifier encrypted in the data field in a manner known in itself, or set up an encrypted circuit-switched connection 7 to the telecommunication server 5 and sent his/her user identifier via this connection. In the telecommunication server 5, the message received is decrypted and the first telecommunication connection 6 is related to the user's account or other record associated with the user. At intervals, the telecommunication server 5 checks whether the telecommunication connections 6, 7 are active and maintains call duration counters based on these checks.

In an example, the payments for the chargeable services offered via the Internet are charged as follows. Using a service-specific counter in the telecommunication server, in which case the customer is charged e.g. on the basis of duration of connection, the customer sends a fixed sum, which is stored in the counter. When the first telecommunication connec-

tion 6 in the open network is set up, the counter is started, and when the counter detects that the stored fix sum has been exhausted, the first telecommunication connection 6 is disconnected. After this, the customer is billed by this fixed sum. In another example, the connection time is paid for via continuous time charging, in which case the server has a service-specific counter which increases the sum to be charged until the user sends the server 5 a request to disconnect the telecommunication connection 6. After this, the customer is billed by the sum indicated by the counter. A request to cancel the service is sent via the second telecommunication connection 7.

In a third alternative, the product or service is presented to the customer via the first telecommunication connection 6, and after the customer has decided to buy, he/she uses the second telecommunication connection 7 to pay for the product or service. Based on the payment, the product or service is delivered to the customer. In a fourth example, the product or service is paid via a mobile station. Using a mobile telephone 4 and a second telecommunication connection 7 in any one of the ways described above, the customer reserves a given sum on his/her account, and the service provider is notified of the reserved sum via the telecommunication server. Based on this notification, the service provider can deliver the product or service to the customer and the customer acknowledges receipt of the product after accepting the delivery. It is to be noted that in all the above examples the state of the payment can be displayed for the customer in real time using the first telecommunication connection 6 and the computer 2.

The invention is not restricted to the examples of its embodiments described above, but many variations are possible within the scope of the inventive idea defined by the claims.

CLAIMS

1. Procedure for setting up a secure service connection in a telecommunication system comprising a first telecommunication network (1), a first terminal device (2) connected to the first telecommunication network, a second telecommunication network (3), a second terminal device (4) connected to the second telecommunication network, and a telecommunication server (5), in which procedure the first terminal device is connected via a first telecommunication connection (6) to the telecommunication server and the second terminal device is connected to the telecommunication server via a second telecommunication connection (7), characterised in that

the unique address of the first terminal device (2) and the data needed for the verification of information giving the first terminal device (2) access to the services of the telecommunication server (5) are transmitted via the second terminal device (4);

the data sent by the second terminal device are verified in the telecommunication server; and

the first telecommunication connection (6) from the telecommunication server to the first terminal device is set up based on the verification and the address data received if the first terminal device has the required right of access to the services of the telecommunication server.

2. Procedure as defined in claim 1, characterised in that a secure telecommunication connection (7) is set up between the second terminal device and the telecommunication server (5) by encrypting the data transmitted via the connection using a predetermined encrypting algorithm.

3. Procedure as defined in claim 1, characterised in that the second telecommunication

connection (7) is set up as a message switching connection which is used to transmit encrypted message packets.

4. Patient's respiration air as defined in any one of claims 1 - 3, characterised in that the message switching connection is used to transmit SMS and/or ESMS messages according to the GSM standard.

5. Procedure as defined in any one of claims 1 - 4, characterised in that a check is carried out in the telecommunication server (5) to establish whether the first and/or the second telecommunication connection (6, 7) is active and whether the user has a right of access to the services provided via the telecommunication server.

6. Procedure as defined in any one of claims 1 - 5, characterised in that, in the telecommunication server (5), the duration of the first telecommunication connection (6) between the first terminal device and the service is measured and the user of the second terminal device (2) is charged on the basis of the duration.

7. Procedure as defined in any one of claims 1 - 6, characterised in that a fixed payment for the service is sent via the second telecommunication connection (7), on the basis of which the telecommunication server (5) disconnects the first telecommunication connection on expiration of the service time corresponding to the payment.

8. Procedure as defined in any one of claims 1 - 7, characterised in that

a purchase order is transmitted via the first telecommunication connection;

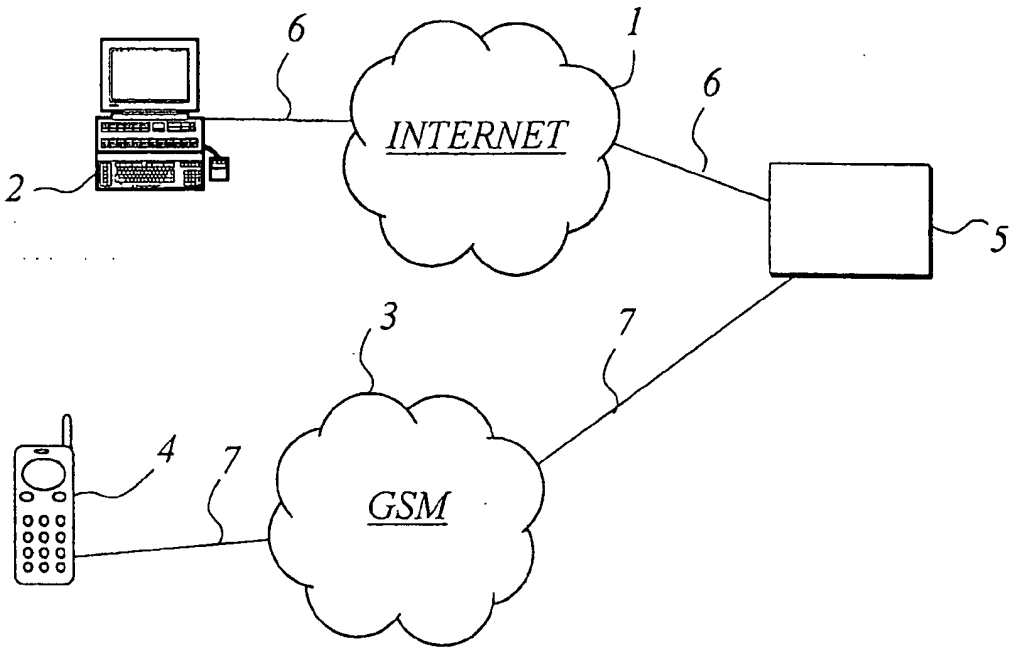
the purchase price is reserved on the user's account via the second telecommunication connection;

the telecommunication server (5) is informed of the reservation; and

the transaction is acknowledged via the second telecommunication connection by the customer.

9. Procedure as defined in any one of claims 1 - 8, characterised in that the first telecommunication network (1) is a data network and the first terminal device (2) comprises means for connecting the terminal device to the data network.

10. Procedure as defined in any one of claims 1 - 9, characterised in that the second telecommunication network (3) is a telephone network and/or mobile communication network and the second terminal device (4) is compatible with the telecommunication network and/or mobile communication network.


6
1
6
INTERNET
2
5
3
7
4
7
GSM